90

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/858,085	05/15/2001	Ali Sheikh	SIDR001USO	2540

48746 7590 12/28/2005

HULSEY IP INTELLECTUAL PROPERTY LAWYERS, P.C.
1250 S. CAPITAL OF TEXAS HIGHWAY
BUILDING THREE, SUITE 160
AUSTIN, TX 78746

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 12/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/858,085	SHEIKH ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-28 and 35-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-28 and 35-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 20, 2005 has been entered.

2. Claims 16-28 and 35-37 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 16-21, 35 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko et al. United States Letters Patent Number 6,789,202 in view of Rothermel et al. United States Letters Patent Number 6,678,827.

As per claim 16:

Ko et al. teach a method for monitoring a security parameter for a network by tracking changes to the contents of system files, the network having a first and a second

server, the first server having a transport mechanism communicatively connected to the second server, the method comprising the steps of:

monitoring at one or more times for changes to a firewall policy; (Col. 6, lines 23-25; global policy can be received from a network security coordinator;) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting on the first server the changes to the firewall policy; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

the second server performing other networking tasks concurrently with the steps of collecting, storing, compiling, or reporting. (Col. 6; lines 39-44; during normal operations of networked computer system, local analyzers receive security information from local sensors)

Ko et al. further disclose a sensor can be constructed from a host-based intrusion detection system (IDS), a network sniffer a firewall or a wrapper that intercepts the arguments of system calls. This makes it possible to reuse existing intrusion detection capabilities on networked computer system in order to implement a system that enforces global intrusion detection policies. (Col. 5, lines 48-52). Furthermore, Ko et al. teach a system that compiles the global policy into local policies for local regions of the networked computer system. Each global policy specifies at least one rule in the form of a local security condition and a local response to be performed to the local security condition and an application program in charge of configuring, monitoring and taking actions involved in providing security within the network. (Col. 1, lines 66-67; Col. 2, lines 1-19; Col. 3, lines 32-40)

Ko et al. do not explicitly disclose a method comprising storing the changes to the firewall policy on the first server; compiling a history of the changes to the firewall policy on the first server; and reporting the history of the firewall policy changes; and

Rothermel et al. in analogous art, however, teach a method comprising

storing the changes to the firewall policy on the first server; (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling a history of the changes to the firewall policy on the first server; (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information; **manager device reads on first server**)

reporting the results from the first server to the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising storing the changes to the firewall policy on the first server, compiling a history of the changes to the firewall policy on the first server, and reporting the results from the first server to the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple network security devices and follow-up its implementation. This way, the firewall policy change can be reported to users such as

system administrators so that they can verify that the firewall policy is correctly implemented.

As per claim 17:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Rothermel et al. further disclose a method comprising the steps of: monitoring whether a change is an approved change; and archiving changes into a first report, the report identifying approved changes. (Col. 5, lines 32-39; as the network security device executes and implements its specific security policy, the network security device gathers network security information about its activities and about the network information that is monitored and forwards it to supervisor devices)

As per claim 18:

Ko et al. further disclose a method comprising the steps of:

monitoring information on an administrator of a networking policy change; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on the administrator of the networking policy changes; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Ko et al. do not explicitly disclose a method comprising archiving one or more sets of information on the administrator; and compiling the one or more sets of information on the administrator of the networking policy changes, the user able to view the compiled information in a format determinable by the user.

Rothermel et al. in analogous art, however, teach a method comprising

archiving one or more sets of information on the administrator; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more sets of information on the administrator of the networking policy changes, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising archiving one or more sets of information on the administrator; and compiling the one or more sets of information on the administrator of the networking policy changes, the user able to view the compiled information in a format determinable by the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple network security devices and follow-up its implementation. This way, the information on the administrator of a network policy change can be reported to users such as system administrators so that they can verify that the administrator of a network policy change is correctly implemented.

As per claim 19:

Ko et al. and Rothermel et al. further disclose a method further comprising the steps of:

monitoring the time of the administrator's networking policy changes; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting the time of the administrator's networking policy changes; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Ko et al. do not explicitly disclose a method comprising archiving one or more sets of times of the administrator's networking policy changes; and compiling the one or more sets of time of the administrator's networking policy changes, the user able to view the compiled time in a format determinable by the user.

Rothermel et al. in analogous art, however, teach a method comprising

archiving one or more sets of times of the administrator's networking policy changes; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more sets of time of the administrator's networking policy changes, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled time in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Rothermel et al. further disclose the network information can also include information about the logging itself, such as a time stamp, the action taken after applying filter rules, and information about the supervisor/host device such as the device name, corresponding process name, and corresponding process ID. (Col. 12, lines 5-9)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising storing the changes to the firewall policy on the first server, compiling a history of the changes to the firewall policy on the first server, and reporting the results from the first server to the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple network security devices and follow-up its implementation. This way, the information on the administrator of a network policy change can be reported to users such as system administrators so that they can verify that the administrator of a network policy change is correctly implemented.

As per claim 20:

Ko et al. and Rothermel et al. further disclose a method comprising the steps of:

collecting the firewall policy change that is pushed (Col. 6, lines 23-25; global policy can be received from a network security coordinator) to the firewall policy; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Ko et al. do not explicitly disclose a method comprising archiving one or more sets of firewall policy information that is pushed to the firewall policy; and compiling the one or more sets of firewall policy information that is pushed to the firewall policy, the user able to view the compiled firewall policy information that is pushed in a format determinable by the user.

Rothermel et al. in analogous art, however, teach a method comprising

archiving one or more sets of firewall policy information that is pushed to the firewall policy; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more sets of firewall policy information that is pushed to the firewall policy, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled firewall policy information that is pushed in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising storing the changes to the firewall policy on the first server, compiling a history of the changes to the firewall policy on the first server, and reporting the results from the first server to the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create

consistent security policy for multiple network security devices and follow-up its implementation. This way, the firewall policy change can be reported to users such as system administrators so that they can verify that the firewall policy is correctly implemented.

As per claim 21:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. and Rothermel et al. further disclose a method further comprising the steps of:

establishing one or more baselines by an administrator for a system on the network; (Col. 6, lines 23-25; global policy can be received from a network security coordinator)

monitoring the one or more baselines established by an administrator; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on changes to the one or more baselines into a baseline report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Ko et al. do not explicitly disclose a method comprising archiving a one or more baseline reports of the changes; and compiling the one or more baseline reports, the user able to view the compiled information in a format determinable by the user.

Rothermel et al. in analogous art, however, teach a method comprising

archiving a one or more baseline reports of the changes; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more baseline reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. to include a method comprising storing the changes to the firewall policy on the first server, compiling a history of the changes to the firewall policy on the first server, and reporting the results from the first server to the user. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy by establishing a baseline for multiple network security devices and follow-up its implementation. This way, the network security information can be monitored and reported to users such as system administrators so that they can verify establishing one or more baseline and its implementation.

As per claim 35:

Ko et al. teach a method for providing a security policy watch comprising the steps of:

pre-configuring standard system alerts that adhere to preexisting corporate security policies; (Col. 4, lines 33-34; Col. 6, lines 39-44)

determining whether a firewall policy complies with pre-existing corporate security policies; (Col. 6, lines 23-25 and lines 36-38) and

Ko et al. further disclose a sensor can be constructed from a host-based intrusion detection system (IDS), a network sniffer a firewall or a wrapper that intercepts the arguments of system calls. This makes it possible to reuse existing intrusion detection capabilities on networked computer system in order to implement a system that enforces global intrusion detection policies. (Col. 5, lines 48-52). Sensor for a firewall policy detection can be implemented on the same structure discussed above in claim 16.

Ko et al. do not explicitly disclose a method comprising generating an alert when a firewall policy is determined not to comply.

Rothermel et al. in analogous art, however, teach a method comprising generating an alert when a firewall policy is determined not to comply. (Col. 3, lines 1-2; Col. 8, lines 23-25)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Ko et al. to include a method comprising generating an alert when a firewall policy is determined not to comply. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple

network security devices and follow-up its implementation. This way, the firewall policy change can be reported to users such as system administrators so that they can verify that the firewall policy is correctly implemented.

As per claim 37

Ko et al. teach a method for monitoring changes made to systems comprising the steps of:

storing scheduled change information in a central database; (Col. 4, lines 33-34; Col. 6, lines 39-44)

detecting actual system changes when they are made to the system; (Col. 6, lines 23-25 and lines 36-38)

transporting actual system change information to a central database; (Col. 4, lines 33-34)

providing for comparison of scheduled change information and actual change information thereby allowing auditors to detect system change errors and system tampering (Col. 5, lines 44-45 and lines 47-49)

Ko et al. do not explicitly disclose a method comprising recording information on scheduled system changes on a central server log.

Rothermel et al. in analogous art, however, teach a method comprising recording information on scheduled system changes on a central server log. (Col. 5, lines 32-39)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Ko et al. to include a method comprising recording information on scheduled system changes on a

central server log. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Rothermel et al. (Col. 4, lines 34-35) in order to create consistent security policy for multiple network security devices and follow-up its implementation. This way, the firewall policy change can be reported to users such as system administrators so that they can verify that the firewall policy is correctly implemented.

5. Claims 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko et al. United States Letters Patent Number 6,789,202 in view of Rothermel et al. United States Letters Patent Number 6,678,827 and further in view of Teng United States Letters Patent Number 5,812,763.

As per claim 22:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the steps of:

monitoring one or more operating system's file integrity on the network; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on changes to the one or more operating system's file integrity into a file integrity report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose a method comprising the step

archiving the one or more file integrity reports; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more file integrity reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

Neither of the references, however, explicitly disclose a method about a file integrity on the network.

Teng in analogous art, however, discloses a system file protection inspector that performs a series of probe operations in connection with protection of each file system to find those which have improper protection levels. (Col. 4; lines 39-43)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. and Rothermel et al. to include a method about a file integrity on the network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Teng (Col. 2, lines 49-50) in order to protect each file by including a protection code. This way, the level of protection is not only at the network level but also includes the files that are stored in each computer that is connected to the network system.

As per claim 23:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the steps of:

monitoring a Web server's configuration file; (Col. 6, lines 23-25; global policy can be received from a network security coordinator;) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on changes to the Web server's configuration file into a Web Server's configuration report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose a method comprising the step

archiving the one or more Web Server's configuration reports; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more Web Server's configuration reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

As per claim 24:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the step of:

monitoring a proxy server's configuration file; (Col. 6, lines 23-25; global policy can be received from a network security coordinator; **computer with global analyzer reads on proxy server**) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on changes to the proxy server's configuration file into a proxy server's configuration file report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose a method comprising the step

archiving the one or more proxy server's configuration file reports; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more proxy server's configuration file reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

As per claim 25:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose comprising the step of:

monitoring a user's password strength; (Col. 6, lines 23-25; global policy can be received from a network security coordinator) (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

collecting information on the password's strength into a password strength report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose a method comprising the step

archiving the one or more password strength report; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more password strength report, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

Neither of the references, however, explicitly disclose a method about a file integrity on the network.

Teng in analogous art, however, discloses a password inspector that detects whether a user who is authorized to use the computer system has selected a password, which can be easily guessed (Col. 4; lines 1-3)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. and Rothermel et al. to include a method about user's password strength on the network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Teng (Col. 4, lines 14-16) in order to protect the network system from unauthorized users. This way, the password strength is checked to avoid easy guessing by another person who is not authorized to use the system.

6. Claims 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko et al. United States Letters Patent Number 6,789,202 in view of Rothermel et al. United States Letters Patent Number 6,678,827 and in view of Teng United States Letters Patent Number 5,812,763 and further in view of Cromer et al. 6,263,441.

As per claim 26:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the step of:

establishing a one or more events that triggers an alert; (Col. 6, lines 23-25; global policy can be received from a network security coordinator)

monitoring for the one or more alert triggering events; (Col. 6, lines 36-38; the system then allows local sensors to implement the specified sensors)

providing an alert notice upon the occurrence of the one or more alert triggering event. (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

Not explicitly disclosed by Ko et al. and Rothermel et al. is that events that triggers an alert.

Cromer et al. in analogous art, however, disclose detecting a change to a configuration of the computer system, using detection logic of the computer, and generating an alert associated with any change in the configuration in real time. (Col. 2, lines 50-64)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. and Rothermel et al. to include a method about events that triggers an alert on the network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Cromer et al. (Col. 2, lines 29-31) in order to provide a method of notifying a remote server when key system components are removed or added or changed to a networked computer.

As per claim 27:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Ko et al. further disclose a method comprising the steps of:

collecting information on the one or more alert triggering event into a alert report; (Col. 4; lines 33-34; local analyzers filter this information and relay it back to global analyzer)

In addition, Rothermel et al. further disclose

archiving the one or more alerts reports; and (Col. 8, lines 23-25; the aggregated network security information can be stored by the manager device)

compiling the one or more alert reports, (Col. 4, lines 43-44; the network security device manager system also allows a manager device to retrieve and analyze the network security information) the user able to view the compiled information in a format determinable by the user. (Col. 3, lines 1-2; the network security information can be displayed to users such as system administrators)

The rationale for combining the above references is the same basis as claim 16 above.

As per claim 28:

Both Ko et al. and Rothermel et al. teach the subject matter as discussed above. In addition, Rothermel et al. further disclose a method comprising the step of: monitoring encrypted secure connections between the first and the one or more second servers. (Col. 5, lines 56-58; any of the information transmitted between the Network security device and the supervisor devices and the manager device can be protected from unauthorized access by encrypting information)

As per claim 36:

Ko et al. and Rothermel et al. teach all the subject matter as disclosed above. Both references do not explicitly disclose whether a system is within certain predetermined corporate guidelines with respect to particular types of software packages, particular versions of specific software, particular hardware, or processor speed.

Cromer et al. in analogous art, however, disclose detecting a change to a configuration of the computer system, using detection logic of the computer, and

generating an alert associated with any change in the configuration in real time. (Col. 2, lines 50-64)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Ko et al. and Rothermel et al. to include a method of determining whether a system is within certain predetermined corporate guidelines with respect to particular types of software packages, particular versions of specific software, particular hardware, or processor speed. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Cromer et al. (Col. 2, lines 29-31) in order to provide a method of notifying a remote server when key system components are removed or added or changed to a networked computer.

Response to Arguments

7. Applicant's arguments, see Remarks, filed October 20, 2005, have been fully considered but are not persuasive. Applicant argues Ko et al. (US 6,789,202) and Rothermel et al. (US 6,678,827) are very broad in their discussions of network security policy and they do not teach the detection and tracking of system changes. The Examiner disagrees with the Applicant and maintains all the rejections. Ko et al. teaches an intrusion detection system for a networked computer system which can be configured dynamically by analyzer to detect specific security-related events and local intrusions within the assigned portion of networked computer system. (Col. 5, lines 40-46; *dynamically detect specific security-related events and local intrusions is the same*

as tracking of system changes). The system compiles the global policy into local policies for local regions of the networked computer system. Each local policy specifies at least one rule in the form of a local security condition for an associated local region of the networked computer system and a local response to be performed in response to the local security condition. (Col. 1, lines 66-67 and Col. 2, lines 1-19) Ko et al. also further disclose an application program in charge of configuring, monitoring and taking actions involved in providing security within networked computer system. And a local intrusion detection component that monitors activity in an assigned portion of networked computer system. (Col. 3, lines 32-40) Rothermel et al. also discloses storing aggregated network security information by the manager device (Col. 8, lines 23-25) and retrieving and analyzing the network security information by the manager device.

In response to applicant's arguments, the recitation "track and report changes to the contents of the system files" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention

where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Ko et al. discloses a policy-driven instrusion detection system by receiving global policy for the network. (Abstract) Rothermel et al. discloses a security manager police device to remotely manage multiple network security devices such as firewall and security applications and a supervisor device that creates and updates the security policy to each of the security devices. In addition, Rothermel et al. further disclose manager device to retrieve, analyze and display all of the network information gathered by the network security devices. (Abstract) One skilled in the art would have been motivated to modify the teachings of Ko et al. with Rothermel et al. in order to create consistent security policy for multiple network security devices and follow-up its implementation. (Col.4, lines 34-35; Rothermel)

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay SG
12/20/05

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER